IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

REMBRANDT PATENT INNOVATIONS, LLC	)	
and REMBRANDT SECURE COMPUTING, LP,	)	
	)	Civil Action No. 2:14-cv-15
Plaintiffs,	)	
	)	**JURY TRIAL DEMANDED**
v.	)	
	)	
APPLE INC.,	)	
	)	
Defendant.	)	
	)	
	)	

REMBRANDT PATENT INNOVATIONS, LLC'S AND REMBRANDT SECURE COMPUTING, LP'S REPLY CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

I. INTRODUCTION

Apple improperly seeks to limit the scope of the claims to certain embodiments, contravening decades of Federal Circuit authority. “There are only two exceptions to [the rule of giving claim terms their plain and ordinary meaning]: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of the claim term either in the specification or during prosecution.” *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371 (Fed. Cir. 2014) (quoting *Thorner v. Sony Computer Entm’t Am.*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)). Apple never shows that either exception applies to justify its limiting constructions.

II. CLAIM CONSTRUCTIONS OF THE DISPUTED TERMS

A. “coupled to”

Apple bases its request to limit “coupled to” to a direct link on the incorrect allegation that each of the six times the term appears in the claims corresponds to a direct connection in the specification. Opp. 21. Claim 1’s recitation of “a trusted repository coupled to said expansion bus” (Ex. A[1] at 22:7), however, covers an indirect connection if that repository is a network host (Br. 7-8). Apple dismisses this example by urging the Court to “read [this appearance of ‘coupled to’] in the context of the five other [appearances]” and arguing that the patent discloses an expansion ROM that might have a direct connection. Opp. 23. Figure 2a, however, shows a network host 254 as the trusted repository, which is reached indirectly through a communications interface. Ex. A at 7:7-9; Fig. 1c. Apple provides no justification for construing the claims to exclude an embodiment, which is contrary to law. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1583 (Fed. Cir. 1996) (a construction that reads out a preferred embodiment “is rarely, if

[1] Exhibits A and B cited herein are attached to Rembrandt’s Opening Brief (Dkt. No. 76).

ever, correct and would require highly persuasive evidentiary support").

Nothing in the patent supports Apple's limited reading, nor does the case Apple cites, *PCTEL, Inc. v. Agere Systems*, No. C03-02474, 2006 U.S. Dist. LEXIS 25943, at *19 (N.D. Cal. Mar. 20, 2006). In *PCTEL*, the specification and prosecution history emphasized the need for a direct physical connection, but in this case they do not. Because the same term should be construed consistently in each appearance in the claims, "coupled to" must include indirect connections. *See Fin Control Systems v. OAM, Inc.*, 265 F.3d 1311, 1318 (Fed. Cir. 2001)

B. "boot component"

Apple misquotes Rembrandt's construction to argue that it supports Apple's position that boot components must be "used by the system BIOS." The processor accesses the operating system kernel after executing the system BIOS,[2] but the system BIOS never uses this boot component. The system BIOS transfers control to a layer (i.e., a boot block) that loads the operating system kernel. Ex. A at 2:52-57, 8:12-37. In this context, the operating system kernel is "used by" the boot block rather than the system BIOS. Apple's construction cannot be correct.

Additionally, Apple argues through the use of the term "module" that a boot component encompasses hardware.[3] Specifically, Apple contends the specification refers to "boot components" (Ex. A at 1:53-58) as hardware components such as "expansion card ROMs," "CMOS memory," or "NVRAM." These references in the specification, however, refer to boot-component software stored in a memory, not the memory itself. Indeed, the same passage identifies other boot-component software, such as "BIOS," "boot sector," and "operating system

[2] Apple asserts that claim 1 "states that boot components are accessed *while* the system BIOS is executed." Opp. 14 (emphasis added). The claim actually states boot components are accessed "when" the system BIOS is executed (22:4-6), which Apple admits can mean "after" (Opp. 18).

[3] In its transfer motions, Apple argued that this case only involves software, not hardware components, but its suggested construction of "boot components" including hardware belies that argument.

kernel." To recover a failed boot component through a trusted repository, as recited in claim 1, the boot component must be software. There is no suggestion of a trusted repository that provides replacement hardware parts, such as replacement memory modules, as would be required under Apple's construction.

Apple, moreover, acknowledges this by referring to boot components as software throughout its brief. For example, Apple argues in the "boot component" section of its brief that "expansion ROM" is hardware, but in the next section ("system BIOS") argues that the patent defines firmware to include an "expansion card" and firmware is "a specific kind of software." Opp. 13-15. Similarly, Apple admits in the "trusted repository" section of its brief that "boot components" are "software and/or configuration data," and the purpose of the trusted repository "is to be a repository for replacement boot components." Opp. 7; *see also* Ex. A at 10:44-46 (describing an expansion ROM implementation of a trusted repository that "contains verified copies of the required software").

Apple also ignores that "components" and "boot components" are used interchangeably in the specification as software components. The specification refers to "execution" of these components (Ex. A at 3:26-39)—only software is executed. The patent also describes obtaining a replacement component through an expansion bus (*id.* at 4:48-59, 22:7), but an expansion bus cannot transmit hardware. When the trusted repository is a network host, the patent describes downloading a replacement component (*id.* at 19:42-45), which also requires the component be software. Finally, in one embodiment when a failed component is recovered, the patent describes recovering through a "simple memory copy" (*id.* at 10:58-61), which can only be done for software. A "boot component" must be software.

The prosecution history is in accord. In response to a prior-art rejection, the patentee argued the reference does not "verify all of the software in the bootstrap process," and the "checks have nothing to do with ensuring the integrity of the software contained in the boot process." Ex. B at REMBAPPL00021703-04. The patentee distinguished another prior-art reference because the invention verified "software components" such as "the system BIOS," "expansion ROMs," "the operating system block," and "the operating system kernel." *Id.* at REMBAPPL00021704-05. Apple dismisses this intrinsic evidence by arguing the patentee's use of "component" rather than "boot component" in the specification and prosecution history raised a presumption the two terms have different meanings. The case Apple cites, *CAE Screenplates, Inc. v. Heinrich Fiedler GmbH*, 224 F.3d 1308, 1317 (Fed. Cir. 2000), refers to a presumption that different terms *in a claim* have different meanings. There is no such presumption for the use of interchangeable terms in the specification or prosecution history.

C. "system BIOS"

Apple attempts to limit "system BIOS" to firmware based on a parenthetical note in the specification describing how a prior-art reference implemented "a system BIOS" in firmware. Ex. A at 2:22-23. The statement Apple bases its argument on is neither an express definition nor a clear and unmistakable disclaimer that would limit system BIOS to firmware implementations. The patentee never limited the claimed system BIOS to "firmware." Rather, the patent refers to a portion of system BIOS as "trusted software" in the preferred embodiments (Ex. A at 9:13-15), and the prosecution history calls the system BIOS a "software component." Ex. B at REMBAPPL00021704-05.

The specification, moreover, describes the system BIOS being implemented in a programmable memory. Ex. A at 9:17-21 ("First section 202 and second section 212 can be contained within a single flash ROM, such as the Intel 28F001BX-B which has an 8KB block that can be protected from reprogramming while the remainder of the ROM can be reprogrammed."). While Apple contends firmware "is installed firmly in hardware and cannot easily be modified" (Opp. 15), the BIOS software in the preferred embodiment is not "firmly" stored in memory as portions of the BIOS can be reprogrammed in the memory. *See*, *e.g.*, Ex. A at 9:17-21.

Apple argues that the specification teaches recovering the system BIOS through a "shadowing" process and the system BIOS is not replaced because it is difficult to modify firmware. Opp. 15. The portion of the specification Apple cites, however, explains that recovery of the system BIOS "is a simple memory copy from the address space of the AEGIS ROM 256 *to* the memory address of the failed [system BIOS]," which, according to Apple, could not happen if the system BIOS was firmware. *See* Ex. A at 10:56-61 (emphasis added). Apple's example supports Rembrandt's construction.

D. "a trusted repository"

Apple argues the specification only shows a trusted repository "on a single network host," (Opp. 7), but Rembrandt's brief showed where the specification describes embodiments with "network hosts," and where both the DHCP server 420 and a separate server 420 form a trusted repository 420 (Br. 13). Although Apple concedes that a DHCP server is used to locate a network host in the recovery process, it denies the DHCP server can be another network host in the trusted repository. Opp. 7. This position contradicts the specification and figures, which identify multiple servers 420, including "DHCP servers 420" and "Server 420 (Trusted Repository)." Ex. A at 16:48-49, 17:32. The specification also describes "network hosts 254." *Id.* at 8:57-59.

In addition, contrary to Apple's representation, the specification never states a network host must contain copies of the plurality of boot components.[4] Opp. 7-8. The portion Apple cites only describes recovering a boot component from a network host; it does not require the network host itself contain copies of the plurality of boot components rather than directing the computer system to a location from which to obtain a replacement boot component. When DHCP server 420 is one of multiple network hosts, it does not contain copies of the boot components, but instead refers the computer system to another server 420 from which to obtain a copy of the failed component using TFTP. *See* Ex. A at 16:54-59; 19:36-45; *see also id.* at 16:48.

E. "verifying the integrity"

The patent distinguishes "verifying the integrity" of software components from using non-cryptographic checksums to detect memory failures. Apple's construction, however, conflates these different concepts, but Rembrandt's does not.

The specification teaches a secure boot process guaranteed to end up in a secure state. Ex. A at 6:25-33. No software code is executed unless it is either (1) explicitly trusted, *or* (2) its integrity is verified prior to use. *Id.* When software is explicitly trusted, like the first portion of BIOS in the preferred embodiment, its integrity is assumed to be valid and is not verified. *Id.*; *see also id*. at 7:30-33, 8:45-49. For software whose integrity is not explicitly trusted, the patent requires use of a cryptographic hash to verify the integrity of the software. *Id.* at 4:40-45, 6:14-16, 11:39-41, 20:21-25.

Apple contends the specification discloses using a non-cryptographic checksum to verify a first portion of the BIOS (Opp. 5-6), but the specification teaches the first portion of BIOS is already assumed to be valid and uncompromised because it is explicitly trusted and therefore is

[4] Apple also wrongly contends Rembrandt's proposed construction of the "wherein" clause demonstrates that the trusted repository "contains" replacement components, Opp. 8, yet Rembrandt's construction is "wherein replacement components are *obtained* from a trusted repository."

not verified. Ex. A at 7:30-33, 8:45-49. The checksum applied to the first portion of BIOS in the preferred embodiment just identifies memory failures. *Id.* at 8:48-51, 9:33-35. Non-cryptographic checksums and CRCs "fail to verify the BIOS." *Id.* at 2:52-65; Ex. B at REMBAPPL00021703. The patentee amended "independent claims 1 and 4 . . . to specifically recite that the present invention, unlike the [the cited prior art], provides a means for verifying the integrity of the system BIOS." Ex. B at REMBAPPL00021704. Apple ignores this evidence.

As a final matter, the phrase "using a cryptographic hash" in Rembrandt's proposed construction does not render the limitations of dependent claim 6 superfluous as Apple argues (Opp. 6), because claim 6 (which does not even depend from claim 1) describes a very specific use of a cryptographic hash to verify the integrity of a boot component. Ex. A at 22:30-36. The term "checking" in Rembrandt's proposed construction is used in place of the term of art "verifying" (or Apple's "confirming") to convey the concept that the result may be that the integrity is *not* verified.

F. "means for verifying the integrity of said boot components and said system BIOS"

Claim 1 recites a "means for verifying," and not "means for recovery," yet Apple's brief refers to the "means for recovery" as if that were the claim language. Opp. 9 ("The network host . . . is part of the means for recovery."). The wherein clause concerns recovery, but does not recite the word "means," thus there is a presumption that this clause is not subject to § 112, ¶ 6. *Aloft Media, LLC v. Adobe Systems, Inc.*, 570 F. Supp. 2d 887, 894-95 (E.D. Tex. 2008) (holding "wherein" clause not subject to construction under § 112, ¶ 6). Apple cites *Griffin v. Bertina*, 285 F.3d 1029, 1033-34 (Fed. Cir. 2002), which did not involve § 112, ¶ 6. Rembrandt is not arguing the "wherein" clause is not limiting, only that it is not subject to construction under § 112, ¶ 6.

Apple seeks to insert "automatically" into the "means for verifying" (Opp. 9-10), but it is improper to change the stated function of such an element. *Golight, Inc. v. Wal-Mart Stores, Inc.*, 355 F.3d 1327, 1333-34 (Fed. Cir. 2004). "Automatically" appears nowhere in any claim. Apple failed to distinguish, let alone acknowledge, this Federal Circuit authority cited in Rembrandt's opening brief. Br. 16-17; Opp. 9-10.

G. "wherein integrity failures are recovered through said trusted repository"

Apple asks the Court to insert "automatically" into the claims because "all of the intrinsic evidence indicates that the '678 Patent was directed solely at automatic recovery." Opp. 10. The express language of the claims, however, does not require automatic recovery, and the specification describes embodiments that permit user intervention in the recovery process, which is not "automatic," as Apple's construction requires. *See* Ex. A at 10:21-25. For example, if during the recovery process the trusted repository should become temporarily unavailable, manual intervention may be required depending on the user's security policy. *Id.* Apple's proposed construction improperly excludes these disclosed embodiments.

The cases Apple cited each involved a clear disclaimer of broader scope. *See, e.g., SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1344 (Fed. Cir. 2001) (holding the specification's use of "all embodiments of the present invention contemplated and disclosed herein," was a "broad and unequivocal" disclaimer of scope broader than the disclosed embodiments). Apple identified no disclaimer in the '678 Patent, and using the term "present invention" is not a magic talisman for limiting the claims. *See, e.g., Voda v. Cordis Corp.*, 536 F.3d 1311, 1320-22 (Fed. Cir. 2008) (refusing to import limitations from "the present invention" where the specification did not uniformly refer to the invention as being so limited and the prosecution history did not reveal such a limitation); *Rambus Inc. v. Infineon Techs.*, 318 F.3d 1081, 1094-95 (Fed. Cir. 2003) (refusing to import limitations from the "present invention" when "the remainder of the specification and the prosecution history shows that Rambus did not clearly disclaim or disavow such claim scope").

H. "a host computer"

Apple's proposed construction of "host computer," which appears only in claim 3, imports limitations and excludes a preferred embodiment, both without justification. The limitations Apple seeks to add describe how the host computer is "connected" to "a separate computer system." This is inconsistent with a preferred embodiment in which a host computer (server 420) is indirectly connected to a computer system (client 410) over a network using various "relay agents" and "gateways." Ex. A at 16:42-53; Fig. 4.

I. "Power on Self Test (POST)"

Contrary to Apple's proposed construction, the specification discloses POST as including tests that are not performed by system BIOS. After providing examples of invoking POST, the specifications states, "All of these tests, except for the initial processor self test, are under the control of system BIOS 112." Ex. A at 8:10-11. The antecedent basis for "these tests" is the Power On Self Test. *See id.* at 7:61-64. And Apple recognizes that the disclosed "processor self test" is performed by the processor itself and not system BIOS. Opp. 17 n.7. Thus, the specification discloses a POST test (*i.e.*, the initial processor self test) that is not performed by system BIOS and would be improperly excluded under Apple's construction.

The declaration Apple submitted from its expert is extrinsic evidence that cannot vary or contradict the intrinsic evidence. *Markman v. Westview Instr., Inc.*, 52 F.3d 967, 981 (Fed. Cir. 1995) (en banc). The same is true for the other extrinsic evidence Apple provided.

J. "when said boot component fails, recovering said failed boot component" and "to replace said boot components"

Apple originally proposed "when" meant "at the time" **(**Dkt. No. 72-1 at 65-66**)**, but after receiving Rembrandt's brief showing the lack of support for this interpretation, Apple seeks to change "at the time" to "as soon as." But interpreting "at the time" to mean "as soon as" is contrary to plain English. "At the time" requires simultaneous action, whereas "as soon as" requires immediate action.

Apple argues "as soon as" captures the concept of the "automated verification and recovery procedure" described in the specification (Opp. 18), but Apple's new proposed construction is just another improper attempt to shoehorn a feature of the preferred embodiment—in this case "automatic"—into the claims, and doing so makes the claims with this term inconsistent with certain embodiments. *See supra* Section G. Apple similarly seeks to improperly introduce the word "automatically" in the term "to replace said failed boot component." All of its attempts violate Federal Circuit precedent. *Thorner*, 669 F.3d at 1365; *Vitronics*, 90 F.3d at 1583.

Apple does not dispute whether a "boot component" (Rembrandt) or a "failed boot component" (Apple) is recovered. Opp. 19. Rembrandt submits that its proposed construction more accurately identifies what is being replaced.

K. "secure protocol"

Apple argues the jury will understand "standard" better than "protocol," but Apple articulates no basis for this conclusory allegation. The specification allows the secure protocol to use a "custom" (i.e., non-standard) protocol, which would contradict Apple's use of "standard" in its construction. To reconcile this disparity, Apple seeks to expand the word "standard" to include custom schemes arguing that custom communication is standard because two participants must agree to communicate in some fashion. Equating "standard" and "custom" guarantees juror confusion far in excess of understanding "protocol." Further, the jury may understand "standard" in many other ways, including as referring to a protocol approved by a standards organization, which is clearly not intended.

Dated: October 15, 2014

Respectfully submitted,

/s/ Trey Yarbrough
Trey Yarbrough
Bar No. 22133500
YARBROUGH WILCOX, PLLC
100 E. Ferguson St., Ste. 1015
Tyler, TX 75702
(903) 595-3111
Fax: (903) 595-0191
trey@yw-lawfirm.com

Gerald F. Ivey (*pro hac vice*)
E. Robert Yoches (*pro hac vice*)
Richard B. Racine (*pro hac vice*)
Christopher T. Blackford (*pro hac vice*)
FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, LLP
901 New York Avenue, N.W.
Washington, D.C. 20001
(202) 408-4000

Stephen E. Kabakoff (*pro hac vice*)
Anita Bhushan (*pro hac vice)*
Benjamin Schlesinger (*pro hac vice*)
FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, LLP
3500 SunTrust Plaza
303 Peachtree Street, N.E.
Atlanta, GA 30308-3263
(404) 653-6400

Jacob Schroeder (*pro hac vice*)
FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, LLP
3300 Hillview Avenue
Palo Alto, CA 94304
(650) 849-6600

ATTORNEYS FOR PLAINTIFFS
REMBRANDT PATENT INNOVATIONS, LLC
and REMBRANDT SECURE COMPUTING, LP

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this 15th day of October, 2014. All other counsel not deemed to have consented to service in such manner will be served via facsimile transmission and/or first class mail.

/s/ Trey Yarbrough
Trey Yarbrough